



Proactive Computer Network Defense and Information Assurance

ONR Program Code 31

November 2010

At a Glance

What is it?

■ The Proactive Computer Network Defense and Information Assurance (CND/IA) prototype will aide the warfighter in identifying and mitigating real-time threats while ensuring continuity of essential operations and access to assured data during attacks.

How does it work?

■ The new cyberdefense architecture will have three main integrated critical components: sensors and gateways, security-enabled protocols and a common operational security decision system. Dynamically reconfigurable and located throughout the network, sensors and gateways will provide enhanced anomaly detection capabilities and robust security features to aid in heightening threat awareness as part of the decision support system. Hardened and dynamic, security-enabled protocols will ensure data delivery and provide configuration and control of network-based security components. To support integrated decision-making for network warfare, a common operational system will aggregate, correlate and visualize the network security posture information, and provide automated decision support to dynamically manage the sensors and gateways.

What will it accomplish?

■ CND/IA will provide cybersecurity situational awareness to support cyber-physical and computer network operations. It will enable the warfighter to understand and quantify the network security posture to support mission planning and mission outcome, and provide a capability to dynamically control network security components to address changing threat environments.

Point of Contact

Stanley Chincheck
(202) 767-2932
stanley.chincheck@navy.mil

Achieving cyberspace information superiority is mission-critical to the Department of the Navy. The current concept—“keep the adversary out”—has failed against sophisticated adversaries. The increasing complexity and quantity of malware, and the emergence of new technology and user risks, present a constant challenge. Unfortunately, the network defense tools and capabilities that currently address these threats are reactive and inflexible, focus on configuration management, and do not allow for a real-time response capability. These tools do not provide intelligent decision aids essential to combating the threat.



To close these gaps, this Office of Naval Research (ONR) CND/IA program will provide the warfighter with a comprehensive, holistic approach to computer network defense. It moves away from traditional concepts of patch management and computer resource management and mitigates real-time threats while ensuring continuity of essential operations and access to assured data during attacks.

The architecture being sought is predicated on providing capability at the lowest level up through the data processing level—including functions such as correlation and fusion that are required to provide decision support and near real-time network-based asset control with an “on-the-fly” engagement capability. The approach focuses on providing automated proactive capabilities that are based on near real-time decision support, as opposed to traditional operator-based “cyber slow” reactions and/or forensics based actions, to address cyber activities as they occur/unfold in the network. The three critical system building blocks of this new architecture include next generation sensors and gateways, next generation security protocols and security management protocols and common operational security decision system.

Research Challenges and Opportunities:

- Algorithms for the detection of malware embedded in binary data files and for the incorporation into sensors and gateways that can distinguish between legitimate network traffic communications and malicious network traffic communications
- Automated decision aides necessary to support automated resource management, generation of recommended courses of action, and the ability to identify and isolate compromised assets from the network
- Security-enabled protocols that provide network-based configuration and control of security components
- Methods and techniques to determine the topology and activity of networks and to use the information provided by attribution data to geo-locate the sources and targets of suspicious network activity
- Methods and techniques for real-time visualization of large sets of network data that are obtained from disparate sources